IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA

HUNTINGTON DIVISION

UNITED STATES OF AMERICA

v. **Criminal No. 3:22-cr-00087**

ALEX KAI TICK CHIN

MEMORANDUM IN SUPPORT
OF DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

The known facts of the matters leading up to the March 21, 2022, seizure of the defendant's Samsung Galaxy 9 smartphone and the two basic searches conducted by the border patrol officers of that device have been set forth in the Defendant's Motion to Suppress. Those searches, which ultimately led to the discovery of the charged images of child pornography produced by Minor Female 1, were illegal in light of the Supreme Court's decision in *Riley v. California,* 573 U.S. 373 (2014), and violated the defendant's Fourth Amendment rights in a variety of ways.

First, the conducting of a basic search of a smartphone at the border, without reasonable suspicion of some form of digital contraband being present on the device, does not serve to advance the intended purposes of the border search exception to the Fourth Amendment warrant requirement. Second, the defendant's Fifth Amendment rights were violated when he was asked questions about an image of a suspected minor while he was handcuffed to a bench awaiting reentry into the United States. Third, the application for search warrant submitted by HSI did not contain any

information that was not independently derived from information other than was gained through the searches of the smartphone. As a result of these violations, this Court should proceed to grant this defendant's Motion and preclude introduction of the evidence outlined in the defendant's Motion which the Government would rely upon for proof of the three counts set forth in the Second Superseding Indictment.

ARGUMENT

(1) The Supreme Court's decision in *Riley v. California* would support the finding that searches of smartphones are "nonroutine" and that border patrol officers must at least have reasonable suspicion that there is some form of digital contraband present on the smartphone in order to seize and conduct a basic search of its contents.

As a general rule, the Fourth Amendment requires that law enforcement searches of property be accompanied by a warrant based upon probable cause. One of the recognized exceptions to this longstanding doctrine covers searches conducted at border crossings. The reasons supporting the border search exception extend from recognizing significant sovereign interests to protect national security, preventing the entry of unwanted persons, regulating the collection of duties, and preventing the introduction of contraband. *United States v. Aigbekaen*, 943 F.3d 713, 720; citing *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004); *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). The border search exception allows designated border patrol officers to conduct what are considered "routine" searches and seizures of persons and property without a warrant or any individualized suspicion. *Aigbekaen*, 943 F.3d at 720 (4th Cir. 2019); *United States v. Kolsuz*, 890

F.3d 133, 137 (4th Cir. 2018). This exception takes into consideration that an individual's expectation of privacy is less at the border than it is in the interior of the country. *Flores-Montano*, 541 U.S. at 154.

The border search exception does have limitations. As relevant here, it still requires that officers have reasonable suspicion to engage in "nonroutine" searches, such as those involving strip searches, body cavity searches or involuntary x-ray searches of persons. *De Hernandez*, 473 U.S. at 541, n.4. Those types of searches implicate significant "dignity and privacy interests." *Flores-Montano,* 541 U.S. at 152. The Fourth Circuit has previously held that a forensic search of a person's cell phone seized at the border must be treated as a nonroutine border search which requires some form of individualized suspicion. *Kolsuz*, 890 F.3d at 145-146.[1] In *Aigbekaen*, the Fourth Circuit clarified that at a bare minimum, the "familiar reasonable suspicion" standard would be needed to justify a warrantless forensic search of a cell phone seized at a border crossing. 943 F.3d at 723.

The Fourth Circuit's decisions in *Aigbekaen* and *Kolsuz* cited the Supreme Court's seminal decision in *Riley v. California*, 573 U.S. 373 (2014), as the basis for categorizing forensic searches of digital devices at border crossings as being non-routine. *Id.* at 145. *Riley* established the legal principle that law enforcement needs to first obtain a warrant in order to search the digital contents of any cell phone

[1] The forensic search conducted in *Kolsuz* was attaching the cell phone to a Cellebrite Physical Analyzer, which conducted an advanced logical file system extraction of the contents of the device. *Id.* at 139. That technique was not used by the border patrol officers or the two HSI agents on the defendant's smartphone on March 21, 2022.

possessed by a defendant at the time of arrest. The underlying facts in *Riley* did not involve law enforcement utilizing the type of intrusive forensic analysis which was undertaken in *Aigbekaen* and *Kolsuz*. Instead, the Court's focus was on the appropriateness of the conduct of law enforcement officers engaged in a basic visual search of the suspect's cell phones, as the border patrol officers did in the defendant's case.

In *Riley*, one of the defendants had been arrested for possession of concealed firearms. 573 U.S. at 378. The defendant's cell phone was taken incident to his arrest for that offense. *Id.* The officer opened the phone and reviewed several text messages which the officer believed contained gang lingo. *Id.* A detective later examined the defendant's phone looking for pictures of gang involvement and found pictures of the defendant standing in front of a car which was thought to have been involved in a shooting. *Id.* The defendant was ultimately charged in connection with shooting incident. *Id.* The second defendant in *Riley* had his flip phone seized after being arrested for selling drugs. *Id.* at 380. The officers who arrested the second defendant had opened the phone to access its call log and looked for a particular number. *Id.*

In *Riley*, the Government argued that the seizure and search of the cell phone fell within the search incident to an arrest exception. *Id.* at 385. The Supreme Court first addressed whether the application of that specific exception in instances involving searches involving cell phones would be consistent with the stated justifications for having a search incident to an arrest exception. *Id.* at 385-391. Those two justifications, concerns for officer safety and the prevention of the

destruction of evidence, were found not to be present to justify the warrantless search of a cell phone. *Id.* First, the digital data contained on a cell phone cannot be used as a weapon to either harm an officer or to secure his arrest. *Id.* at 387. Second, officers have the ability to secure a cell phone from a suspect to eliminate any risk that the suspect would delete incriminating information before a warrant could be obtained. *Id.* at 388.

The Court went on to discuss the privacy-related concerns associated with cell phones and how they differed from other objects which might be found on a suspect's person. *Id.* at 392-395. First, the immense storage capacities of modern cell phones allow large volumes of information and data to be kept within the device. *Id.* In 2015, the current top selling smartphone had a capacity of 16 gigabytes, which translates into millions of pages of text, thousands of pictures, or hundreds of videos. *Id.* at 394. Cell phones collect many distinctive types of personal information, such as addresses, phone logs, banking information, within one place. *Id.* The sum of an individual's private life can be reconstructed through the information contained on a cell phone. *Id.*

Second, the Court noted the pervasiveness in which most Americans use and rely upon cell phones as part of their daily lives. *Id.* at 447. It is now the person who does not have a cell phone who is the exception from the norm. These phones automatically store information, such as internet browsing history and GPS data,

which reveal the person's private interests.[2] *Id.* at 448. In reaching the conclusion that warrants were required for searches of cell phones, the Court recognized that the decision would necessarily have an impact on law enforcement's ability to combat crime. *Id.* at 401. However, "[P]rivacy comes at a cost," and the information contained within cell phones can still be discovered, but with the requirement of a judicially approved search warrant. *Id.*

The Fourth Circuit's decisions in *Aigbekaen* and *Kolsuz* relied upon *Riley* as the basis for finding that intrusive forensic analysis of smartphones seized at the border requires some measure of individualized suspicion. In *Aigbekaen*, Homeland Security Investigations ("HIS") had received a report from a minor that the defendant had been trafficking her for sex in three states. 943 F.3d at 717. HSI submitted a request to U.S. Customs and Border Protection to seize any electronic devices that the defendant may have in his possession upon his return to the United States. *Id.* The defendant's laptop computer, iPhone, and iPod devices were seized and forensically searched, which ultimately uncovered information relating to sex trafficking.[3] *Id.* at 718. There were no manual or basic searches initially conducted on these devices, and the defendant's challenge was to the legality of the forensic searches as falling outside of the border search exception. *Id.*

[2] The average smartphone in 2015 had 33 installed applications which together can form a "revealing montage of the user's life." *Id.*

[3] The forensic search entailed connecting external equipment in order to unlock the entire contents of the devices, including password protected files and restoring deleted materials. *Aigbekaen*, 943 F.3d at 718, n.2.

The Fourth Circuit initially noted that the border search exception would not excuse a warrantless search where applying that exception "would untether the rule from the justifications underlying it." *Id.* at 720; citing *Riley*, 573 U.S. at 386. The purposes behind the border search exception serve to protect national security interests, collecting duties, preventing the entry of unwanted persons and disrupting efforts to export or import contraband. *Id.* at 721; citing *United States v. Ramsey*, 431 U.S. 606, 620 (1977). Where a non-routine search becomes too "attenuated" from these justifications, the search will no longer be covered by the border search exception. *Id.* at 721.

As a result, the Government could not invoke the border search exception on behalf of the generalized interest in law enforcement and combatting crime. *Id.* citing *Kolsuz*, 890 F.3d at 143. While HSI may have had probable cause to suspect that the defendant had committed "grave domestic crimes," those suspicions were completely separate from the sovereign interests pertaining to the border search exception. *Id.* Moreover, it would be "patently unreasonable to permit highly intrusive forensic searches of travelers' digital devices" without warrants on grounds unrelated to the border search exception. *Id.* at 722. The Court further rejected the Government's argument that a warrantless forensic search was permitted out of concern that evidence of child pornography might be present on the defendant's devices. *Id.* at 723. Even if this type of search was justified by reasonable suspicion, the Court found no "particularized and objective basis" for the HSI agents to reasonably suspect that the defendant possessed child pornography. *Id.* Although the warrantless forensic

searches were found to have violated the defendant's Fourth Amendment rights, the Fourth Circuit found that the evidence was preserved through the good faith exception as at the time of the seizure of the devices in 2015, there was no established binding precedent which prohibited warrantless border searches of digital devices. *Id.* at 725; citing *Kolsuz,* 890 F.3d at 148. For purposes of the defendant's case, the Government is not entitled to rely upon a good faith exception given the nature of the significant privacy interests recognized at border crossings in the *Aigbekaen* and *Kolsuz* decisions.

(2) This Court should find that there is no real distinction in the severity of a breach of an individual's privacy rights between an officer browsing through open applications on a seized smartphone versus submitting the device for forensic analysis.

The Fourth Circuit in *Aigbekaen* did not discuss whether the interests underpinning the border search exception would cover basic searches of electronic devices by border patrol officers. *Id.* at 723. The issue was not addressed by the Fourth Circuit in *Kolsuz* as the defendant did not raise a challenge to the manual search of his phone conducted at the airport. 890 F.3d at 140, n.2. The First, Ninth, and Eleventh Circuits have held that basic searches of electronic devices at the border are considered to be "routine" and need not be supported by reasonable suspicion.[4] The First Circuit's decision in *Alasaad* noted that there was a 2018 Border Patrol Policy which allows their agents to conduct a basic search of any electronic device with or without reasonable suspicion. 988 F.3d at 13. Advanced searches of electronic

[4] *See Alasaad v. Mayorkas*, 988 F.3d 8, 19 (1st Cir. 2021); *United States v. Cano*, 934 F.3d 1002, 1016 (9th Cir. 2019); *United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018).

devices with forensic software require supervisory approval and can only be conducted in instances where there is reasonable suspicion of a crime being committed or a national security concern. *Id.*

These decisions, as well as any Border Patrol Policy statement which the Government would rely upon, have overlooked the privacy protections afforded to individuals possessing smartphones under *Riley*. Moreover, the justifications supporting the border search exception are not necessarily satisfied given the facts involved with the defendant's case. First, the defendant's status as a registered sex offender, by itself, would not warrant any reasonable suspicion for an officer to conduct an investigative stop or check the contents of any smartphone which he possessed. *See United States v. Black*, 707 F.3d 531, 540 (4th Cir. 2013); *United States v. Foster,* 634 F.3d 243, 246-247 (4th Cir. 2011); *United States v. Sprinkle*, 106 F.3d 613, 617 (4th Cir. 1997). The Fourth Circuit has made it clear that an officer has to have more than just prior knowledge of a suspect's criminal record in order to demonstrate that there was a reasonable suspicion of the suspect's involvement in ongoing criminal activity. *Id.*

Second, the border patrol officers had no information which suggested that the defendant had engaged in any criminal conduct during the brief period of time that he had spent in Mexico. There is no indication that the defendant's name was present on any list of persons whom HSI considered as a potential threat to national security. Finally, the defendant was traveling alone, on foot, and passed through the same port of entry only an hour or two before. There were no cars or luggage which required

further inspection to check for contraband upon the defendant's return. Given the brief time which the defendant spent in Mexico, there was no information to suggest to a reasonable border patrol officer that the defendant's smartphone would contain any form of digital contraband.

Even though a smartphone is placed in "airplane mode" to block any connection with the Internet, a wide variety of personal information already stored within the applications becomes open for inspection. This would include recent email traffic; calendar entries; photos/videos maintained in a gallery application; personal reminder notes; contact phone numbers and addresses of friends/family; names of contacts through Facetime; text messages with others; conversations within mainstream social media such as Facebook, Snapchat, WhatsApp, and Remind; books being read through Kindle; and personal financial information through Mint.

Given the sheer amount of personal information which is present on today's smartphones, the defendant's privacy rights should be recognized to at least require border patrol officers to demonstrate reasonable suspicion of the presence of digital contraband before any smartphone can be seized and subjected to a basic search at border crossings.

(3) A reasonable person in the defendant's position would have thought he was not free to leave the secondary inspection area, and he should have been advised of his *Miranda* rights before any questions were asked about any images observed on his smartphone.

The test for determining whether an individual is "in custody" for *Miranda* purposes is whether, under the totality of circumstances, the "suspect's freedom of

action is curtailed to a degree associated with an arrest." *Berkemer v. McCarty,* 468 U.S. 420, 440 (1984); *United States v. Leggette*, 57 F. 4th 406, 410 (4th Cir. 2023). In the context of a border crossing, courts have held that an arrest occurs when "a reasonable person would believe that he is being subjected to more than temporary detention occasioned by border crossing formalities." *United States v. Price*, 980 F.3d 1211, 1225 (9th Cir. 2020); *See also United States v. Ventura*, 85 F.3d 708, 710-711 (1st Cir. 1996).

The first factor of the two-part test for determining whether *Miranda* warnings are to be given includes determining whether a reasonable person in that situation would have felt that he or she was not free to stop the questioning and leave. *Leggette*, 57 F.4th at 410. This factor was clearly met, as one of the defendant's arms was handcuffed to a bench after his smartphones were taken to be searched. The defendant further had to await the approval of the border patrol officers to leave the port of entry and resume his travel in the United States. The defendant remained handcuffed to the bench for several hours until HSI agents told him that he was now free to go, but HSI was keeping his two smartphones.

The second factor evaluates whether the relative environment where the questioning occurs presents the same type of inherent coercive pressures as one would find in a police station. Once the defendant was taken into a secondary inspection area, he was treated like a suspect in a criminal case and handcuffed to a bench. The questions about the suspected underaged female were asked while the defendant remained handcuffed. The questions did not serve any purpose in the

border patrol's assessment as to whether the defendant would be allowed reentry. Rather the purpose would have been to develop information that would be useful in a subsequent criminal prosecution given their observation of an image of the suspected underaged female's breasts. Given these factors, the overall environment to which the defendant was subjected would have been similar to any holding area where only law enforcement officers had the ability to freely go between rooms. This Court should find that the border patrol officers should have acted in the same manner as the two HSI agents and provided *Miranda* warnings before asking any questions about the contents of the smartphone.

(4) The operation of the exclusionary rule would prohibit all evidence which was acquired as the direct or indirect result of an illegal search.

The Fourth Circuit has held that a district court evaluating whether unlawfully obtained information "affected the decision to issue the warrant" should "examine the search warrant affidavit absent the illegally obtained information to determine whether the untainted portion of the affidavit set forth probable cause." *United States v. Walton*, 56 F.3d 551, 554 (4th Cir. 1995). The March 25, 2022, warrant issued for the search of the defendant's smartphone relied entirely upon the results of illegally obtained evidence resulting from the two basic searches of the device conducted by the border patrol officers and the two HSI agents. (Ex. A, Bates Nos. Chin - 0049-0051). The submitted affidavit provided a detailed description of the contents of observed photos and text messages found on the defendant's smartphone. *Id.* The follow up investigative work to locate the whereabouts of Minor

Female 1 was not the result of any independent source. This was an undertaking accomplished by the image of her face, her full name and Snapchat screen names observed in the defendant's Snapchat application. Clearly, this unlawfully obtained evidence served as the sole factual basis for the issuance of the search warrant.

The exclusionary rule prohibits the admission of evidence that is acquired as a direct or indirect result of an illegal search. *United States v. Mowatt*, 513 F.3d 395, 403 (4th Cir. 2008). Where there was no reasonable suspicion to justify the initial seizure and search of the defendant's smartphone, and no factual basis supporting a probable cause determination for the issuance of the search warrant, all subsequently obtained evidence, either tangible or testimonial, obtained as a direct result of an illegal search should be excluded as fruit of the poisonous tree. *See Utah v. Strieff*, 579 U.S. 232, 237-238 (2016); *United States v. Terry*, 909 F.3d 716, 720 (4th Cir. 2018).

For the reasons set forth herein, as well as in the accompanying Motion to Suppress, the defendant respectfully moves for the entry of an appropriate Order granting the defendant's Motion and precluding the Government from introducing any forensic evidence concerning the contents of the defendant's Samsung Galaxy 9 smartphone as well as the anticipated testimony of Minor Female 1 concerning her prior communications with the defendant.

Respectfully submitted this 6th day of March, 2023.

ALEX KAI TICK CHIN

By Counsel

WESLEY P. PAGE
FEDERAL PUBLIC DEFENDER

s/David R. Bungard
David R. Bungard, Bar Number: 5739
Assistant Federal Public Defender
Office of the Federal Public Defender
300 Virginia Street, East, Room 3400
Charleston, West Virginia 25301
Telephone: (304) 347-3350
Facsimile: (304) 347-3356
E-mail: david_bungard@fd.org